Centre Plans Stronger Defences for Key Data

The Ministry of Home Affairs has directed the National Information Security Policy and Guidelines (NISPG) to upgrade and update its policies to secure government data and control access to it.

Why there is a need for upgradation of NISPG?

- The sensitive information making its way into the Internet has added to the vulnerability of information sharing. Earlier the files were locked in a cupboard and accountability could be fixed, but with the advent of Digital India, a number of issues were in a grey area.
- The new policy would take into account the evolving cyberspace and the overall policing system in the country.
- The new policy would cover issues pertaining to the Official Secrets Act.
- There are issues relating to physical security of a computer, for example whether the hard disk will be destroyed before a computer is discarded.
- There are issues relating to the network as well. If information is riding on own cyber cable, then everything can be encrypted, but if it is riding on a commercially available one, then one will have to make sure that guidelines are complied with.
- The threats had to be recognised and the measures were to be updated accordingly.

Objectives of National Information Security Policy and Guidelines

- These guidelines are based on the analysis of existing global security standards, and frameworks; and the emerging trends and discourse in the wake of persistent threats, and cyber-attacks on critical infrastructure of nations globally.

- The scope of these guidelines encompasses Government and Public Sector organizations and associated entities and third parties, for protecting the information under their control or ownership during information's life-cycle including creation, storage, processing, accessing, transmission, destruction etc.
- The objective of these guidelines is to improve the information security posture of an organization possessing any information, including classified information, and does not restrict organizations from adopting additional stringent practices over and above these guidelines.
- Organizations may evaluate various additional measures for the security of information they possess for protecting their information depending upon the sensitivity, criticality and importance of such information in the overall Internal Security and National Security interest of the country.